Foro Regional de la UIT para las Américas sobre Ciberseguridad

- Conectar el mundo responsablemente -

Santo Domingo, República Dominicana
23-25 de noviembre de 2009

RESULTADOS DEL FORO

Al concluir el **Foro Regional de la UIT para las Américas sobre Ciberseguridad**, los participantes destacaron los siguientes aspectos:

- Coincidieron en que la **ciberseguridad era una cuestión de alcance mundial**, que requiere cooperación transfronteriza. En este sentido, se han de tomar medidas en los planos tanto nacional como regional y mundial a fin de hacer frente a los distintos aspectos de las ciberamenazas y de proteger las infraestructuras esenciales.
- Hicieron hincapié en que la importancia creciente de la ciberseguridad para todos los países de la Región de las Américas, y en que los gobiernos tenían que estar debidamente informados y coordinados en esta materia.
- Reconocieron la utilidad de la **Agenda sobre Ciberseguridad Global (ACG)** como mecanismo y marco para la cooperación internacional en materia de ciberseguridad, y alentaron a los países a emprender actividades relacionadas con las cinco áreas de trabajo de la ACG (1. Medidas legales; 2. Medidas técnicas y de procedimiento; 3. Estructuras institucionales; 4. Creación de capacidades; y 5. Cooperación internacional), así como a compartir con otros países de la región sus experiencias en la puesta en práctica de tales iniciativas en el plano nacional.
- Confirmaron la utilidad del **Foro regional sobre Ciberseguridad** como plataforma para que pudieran reunirse representantes de países y de organizaciones regionales e internacionales a fin de discutir y desarrollar medidas concretas destinadas a crear capacidad y competencia en la región en materia de ciberseguridad.
- Se mostraron de acuerdo en que una **respuesta nacional coordinada en materia de ciberseguridad** requería la participación de todos los actores pertinentes e incluía la sensibilización e implicación a todos los niveles. A todos los actores les corresponde desempeñar un papel, y es fundamental que el gobierno asuma la responsabilidad para la coordinación de la respuesta nacional. A este respecto, instaron a los países de la región a compartir tanto información y experiencias como prácticas idóneas, y a estudiar posibles alianzas para lograr respuestas efectivas en materia de ciberseguridad, y afirmaron la necesidad de promover la aplicación de las normas internacionales con el fin de garantizar la interoperabilidad entre las distintas soluciones de ciberseguridad que se están utilizando. Sólo podrá responderse a los desafíos mundiales a través de la colaboración en lo que atañe a la formulación de estrategias, la definición de prácticas óptimas, la elaboración de normas y la aplicación de soluciones concretas.
- Destacaron la necesidad de **crear capacidad** en los distintos ámbitos de la ciberseguridad, y alentaron a los países a que integraran, dentro de sus esfuerzos nacionales de ciberseguridad, iniciativas destinadas a proteger a los menores en línea, y a que participaran en actividades e iniciativas regionales y mundiales, como por ejemplo la iniciativa Proteger a la Infancia en línea (PIeL).

- Señalaron que la realización de una **autoevaluación nacional de la ciberseguridad**, utilizando herramientas y materiales existentes, como la Herramienta de la UIT para la autoevaluación nacional de la ciberseguridad/CIIP, podía resultar de utilidad para los países a efectos de contribuir a determinar la situación de los distintos actores nacionales en lo que se refiere a su disposición y preparación en materia de ciberseguridad; qué es lo que están haciendo y lo que podrían hacer después y, como resultado de todo ello, definir futuras medidas prácticas con miras a la formulación de una estrategia nacional de ciberseguridad.
- Se comprometieron a adoptar medidas en relación con la **formulación de una estrategia nacional de ciberseguridad** y a asegurarse de que se tomara en consideración la cooperación internacional en el desarrollo de los distintos componentes de la ciberseguridad nacional.
- Observaron la necesidad de que los países compartieran información y prácticas óptimas en el ámbito del **desarrollo de un marco jurídico y el establecimiento de medidas efectivas para velar por el respeto del mismo**. Se mencionó a este respecto la utilidad de algunos recursos y herramientas existentes como, por ejemplo, la guía de la UIT para entender el ciberdelito y la Colección de herramientas para la legislación en materia de ciberdelitos (*Toolkit for Cybercrime Legislation*).
- Expresaron la necesidad de compartir información y de prestarse asistencia mutua en el ámbito del **desarrollo de las capacidades nacionales de vigilancia, alerta y respuesta en caso de incidente** y señalaron que, con el fin de propiciar el desarrollo de las capacidades de ciberseguridad, incluida la creación de EIII nacionales, resultan de utilidad los recursos y servicios que la UIT pone a disposición en colaboración con asociados clave tales como la **Alianza Multilateral Internacional contra las Ciberamenazas (IMPACT)**, los gobiernos y otras partes interesadas de la región, por ejemplo los CSIRT/CERT/EIII nacionales. La labor relativa a las normas de seguridad forma parte de dichos esfuerzos.
- Señalaron la **utilidad de la formación impartida durante el Foro en tres ámbitos principales**: formulación de una estrategia nacional de ciberseguridad; creación de capacidades nacionales de vigilancia, alerta y respuesta en caso de incidente; y elaboración de legislación destinada a penalizar el uso indebido de las TIC.

Si desea más detalles acerca de este Foro Regional de la UIT para las Américas sobre Ciberseguridad, puede acudir al sitio web en la dirección: www.itu.int/ITU-D/cyb/events/2009/santo-domingo/.

_____